What is claimed is:

Sub A1

1. An electronic authentication method comprising:

generating an identifier for contents in a first information processing apparatus;

storing said identifier in a storage unit;

transmitting said contents and said identifier to a second information processing apparatus;

inputting data for said contents in said second information processing apparatus;

transmitting said input data and said identifier from said second information apparatus to said first information apparatus; and

authenticating legitimacy of said input data and invalidating said stored identifier if said received identifier matches said identifier in said storage unit in said first information processing apparatus.

2. An electronic authentication method according to claim 1, wherein in said first information processing apparatus, said identifier is embedded in said contents prior to transmission of said contents to said second information processing apparatus.

3. An electronic authentication method according to claim 2, said method further comprising:

embedding an encryption key in said contents in said first information processing apparatus prior to transmission of said contents to said second information processing apparatus;

encrypting said input data in said second processing apparatus by using said encryption key prior to transmission of said input data to said first information processing apparatus; and

decrypting said received input data in said first information processing apparatus.

4. An electronic authentication method according to claim 3, wherein: said embedded encryption key is a public key; said received input data is decrypted using a private key associated with said public key; and said public key and said private key are generated in said first information processing apparatus.

5. An information processing method comprising:

generating an identifier for contents;

storing said identifier;

transmitting said contents and said identifier to an external apparatus;

receiving data from said external apparatus;

acquiring an identifier for said contents; and

carrying out processing based on said received data and invalidating said stored identifier if said acquired identifier matches said stored identifier.

6. An information processing method according to claim 5, wherein said identifier is embedded in said contents prior to transmission of said contents to said external apparatus.

7. An information processing method according to claim 6, said method further comprising:

embedding an encryption key in said contents prior to transmission of said contents to said external apparatus; and

receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier.

8. An electronic authentication system comprising a first information processing apparatus and a second information processing apparatus wherein:

said first information processing apparatus comprises:

a means for generating an identifier for contents;

a storage means for storing said identifier; and

a means for transmitting said contents and said identifier to said second information processing apparatus;

said second information processing apparatus comprises:

a means for inputting data for said received contents; and

a means for transmitting said input data and said identifier to said first information processing apparatus; and

there is further provided a processing means for authenticating legitimacy of said input data received by said first information processing apparatus and invalidating

said stored identifier and identifier received by said first information processing apparatus matches said identifier stored in said storage means.

9. An electronic authentication system according to claim 8, wherein said first information processing apparatus further includes an embedding means for embedding said identifier in said contents; and said first information processing apparatus transmits said contents including said embedded identifier to said second information processing apparatus.

10. An electronic authentication system according to claim 9, wherein said first information processing apparatus transmits said contents, said contents further including an embedded encryption key, to said second information processing apparatus; and said first information processing apparatus further comprises a reception means for receiving an identifier encrypted by using said encryption key and decrypting said encrypted identifier.

11. An information processing apparatus comprising:

a generation means for generating an identifier for contents;

a storage means for storing said identifier;

a transmission means for transmitting said contents and said identifier to an external apparatus;

a reception means for receiving data from said external apparatus;

an acquirement means for acquiring an identifier for said contents from said received data; and

a processing means for carrying out processing based on said received data and invalidating said identifier stored in said storage means if said acquired identifier matches said stored identifier.

12. An information processing apparatus according to claim 11, said apparatus further comprising an embedding means for embedding said identifier in said contents, wherein said transmission means transmits said contents including said embedded identifier to said external apparatus.

13. An information processing apparatus according to claim 12, wherein said transmission means transmits said contents further including said embedded

encryption key to sai[redacted]ernal apparatus; and there is further [redacted]ided a reception means for receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier.

14. An information processing apparatus comprising:

a contents requesting means for requesting an external information processing apparatus to transmit contents;

a reception means for receiving said requested contents and an identifier embedded in said contents;

an extraction means for extracting said identifier from said contents;

an input means for inputting data for said contents; and

a transmission means for transmitting said input data and said identifier to said external information processing apparatus.

15. An information processing apparatus according to claim 14, said apparatus further comprising an encryption means for encrypting said input data by using an encryption key additionally embedded in said contents received by said reception means.

16. A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a generation function for generating an identifier for contents;

a storage function for storing said generated identifier;

a transmission function for transmitting said contents and said identifier to an external apparatus;

a reception function for receiving data from said external apparatus;

an acquirement function for acquiring an identifier for said contents from said received data; and

a processing function for authenticating legitimacy of said received data and invalidating said stored identifier if said acquired identifier matches said stored identifier.

17. A storage medium for storing information readable by a computer according to claim 16, said medium characterized in that said information further has a function for embedding said identifier in said contents, wherein said transmission

function transmits said contents including said embedded identifier to said external apparatus.

18. A storage medium for storing information readable by a computer according to claim 17, said medium characterized in that: said transmission function transmits said contents further including said embedded encryption key to said external apparatus; and said information further includes a function for receiving said data encrypted by using said encryption key and decrypting said received encrypted data.

19. A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a contents requesting function for requesting an external information processing apparatus to transmit contents;

a reception function for receiving said requested contents and an identifier embedded in said contents;

an extraction function for extracting said identifier from said contents;

an input function for inputting data for said contents; and

a transmission function for transmitting said input data and said identifier to said external information processing apparatus.

20. A storage medium for storing information readable by a computer according to claim 19, said medium characterized in that said information further includes a function for encrypting said input data by using an encryption key additionally embedded in said contents received by said reception function.

21. An electronic authentication method comprising:

generating an identifier for contents in a first information processing apparatus;

driving said first information processing apparatus to store said identifier and the present time as a storage time in a storage unit;

transmitting said contents and said identifier to a second information processing apparatus;

inputting data for said contents received by said second information processing apparatus in said second information processing apparatus;

transmitting said input data and said identifier to said second information processing apparatus to said first information processing apparatus; and

invalidating said identifier stored in said storage unit if said identifier received by said first information processing apparatus is not stored in said storage unit or a time of a predetermined length has lapsed since said storage time stored in said storage unit.

22. An electronic authentication method, comprising:

generating an identifier for an access to contents in a first information processing apparatus;

storing said identifier in a storage unit;

transmitting said contents and said identifier to a second information processing apparatus;

inputting data for said contents received by said second information processing apparatus in said second information processing apparatus;

transmitting said input data and said identifier from said second information processing apparatus to said first information processing apparatus; and

validating said input data only for this transaction if said identifier received by said first information processing apparatus matches said identifier stored in said storage unit.

23. A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a generation function for generating an identifier for contents;

a storage function for storing said generated identifier in a storage means;

an acquirement function for acquiring an identifier for said contents from said data received from an external apparatus; and

a processing function for carrying out processing based on said received data and invalidating said identifier stored in said storage means if said acquired identifier matches said stored identifier.

24. An authentication method in a system in which a first computer making a request for a service is connected to a second computer rendering services via a network, requested contents being transmitted from the second computer to the first

computer, data being transmitted from the first computer to the second computer associated with the contents, said method comprising:

generating at the second computer an access number for accessing the contents and cataloging the access number in a storage unit;

embedding the access number in the contents so that the access number is invisible and transmitting the contents to the first computer;

displaying the contents at the first computer;

adding the access number fetched from the contents to data inputted associated with the contents and transmitting the inputted data to the second computer; and

authenticating validity at the second computer of the received data when the received access number has been cataloged and invalidating the cataloged access number.

25. An authentication method according to claim 24, wherein the second computer generates a public key and a private key for accessing the contents and catalogs the public key and the private key in the storage unit, embeds the public key in the contents so that the public key is invisible and transmits the contents to the first computer, allows the first computer to encrypt data on inputted associated with the contents by the public key fetched from the contents and transmit the data to the second computer, and decrypt the received data by the public key cataloged when the received access number has been cataloged.

26. A storage medium for storing a program which can be read by a computer, wherein the program has a function of generating an access number for accessing contents requested from the outside, a function of cataloging the generated access number in a storage unit, a function of embedding the access number in the contents so that the access number is invisible and transmitting the contents to the outside, a function of receiving data to which the access number is added from the outside, and a function of authenticating validity on the received data when the received access number has been cataloged and invalidating the cataloged access number.

27. A storage medium for storing a program which can be read by a computer according to claim 26, wherein the program has a function of generating a

public key and a private key for accessing the contents, a function of cataloging the public key and the private key in the storage unit, a function of embedding the public key and the private key in the contents so that the public key is invisible and transmits the contents to the outside, a function of receiving data encrypted by the public key from the outside, and a function of decrypting the received data by the public key cataloged when the received access number has been cataloged.

28. A storage medium for storing a program which can be read by a computer, wherein the program has a function of displaying contents received from the outside, a function of receiving data input associated with the contents, a function of fetching an access number embedded in the contents so that the access number is invisible, and a function of adding the access number to the inputted data and transmitting the data to the outside.

29. A server apparatus comprising:

a processor;

a storage device;

a network interface; and a bus interconnecting said processor, said storage device and said network interface;

wherein said processor generates an identifier for contents and stores said identifier into said storage device; and wherein said processor transmits said contents and said identifier to an external apparatus via said network interface; and wherein said processor receives data from said external apparatus via said network interface; and thereupon acquires from said data an identifier for said contents from said received data; and wherein said processor performs processing based on said received data and invalidates said identifier stored in said storage means if said acquired identifier matches said stored identifier.

30. A server apparatus according to claim 29, wherein in said apparatus, said processor further embeds said identifier in said contents; and wherein said processor transmits said contents including said embedded identifier to said external apparatus.

31. A server apparatus according to claim 30, wherein in said apparatus, said processor further transmits said contents, said contents further including

said embedded encryption key, to said external apparatus; and wherein said apparatus receives an identifier encrypted using said encryption key; and thereupon decrypts said received encrypted identifier.

32. A client apparatus comprising:

a processor;

an input device;

a network interface; and a bus interconnecting said processor, said input device and said network interface;

wherein said processor requests an external information processing apparatus to transmit contents via said network interface; and wherein said processor receives said requested contents and an identifier embedded in said contents; and thereupon, said processor extracts said identifier from said contents; and wherein said processor receives input data for said contents from said input device; and wherein said processor transmits said input data and said identifier to said external information processing apparatus via said network interface.

33. A client apparatus according to claim 32, wherein in said apparatus, said processor further encrypts said input data using an encryption key additionally embedded in said contents received via said network interface.

34. An information processing apparatus comprising:

a means for acquiring a contents from an external information processing apparatus;

a means for receiving the contents;

a means for inputting a data with respect to the contents;

a means for sending the inputted data and an identifier of the contents to the external information processing apparatus; and

a means for displaying that an access is impossible if the contents is accessed at least once.